FRAUD Insights

CHICAGO TITLE®

DATA verification vs. identity document authentication

Recent trends in real estate fraud have made it imperative to authenticate the identity of your sellers to ensure you know exactly with whom you are conducting business. Instances of fraudsters impersonating the identity of property owners — and then listing the property for sale — has been increasing exponentially.

But what is the best way to "know your customer?" With terms thrown around such as verification, validation, authentication, etc., it can be confusing to know what steps need to be taken to ensure you can effectively put a stop to fraud.

Below is a summary of two of those terms – ID Data Verification and Identity Document (ID) Authentication.

How do you verify data on an ID?

ID data can be verified by ensuring the information on the front of the ID (i.e., the printed information, such as name, birthdate, ID number and expiration date) matches what is digitally encoded on the document, whether in the barcode, magnetic strip, machine-readable-zone (MRZ), digital watermark or radio frequency identification (RFID) chip. Making sure data is correct and consistent is just one way you can help prevent fraud in real estate transactions.

Some verification services might additionally send the personal identifiable information (PII) to be compared to public-records data, such as the department of motor vehicle (DMV) records or private identity databases, to make sure the data matches what is on file with the issuing authority for the document.

What is ID Authentication?

By definition, ID Authentication is the process of authenticating the genuineness of the source of the data (e.g., the document). It involves verifying the physical identity document itself for authenticity, rather than just the data contained within it. This ensures that the physical document being presented was genuinely issued by a government agency and not a fake created by a forgery operation.

The difficulty from a transactional perspective lies in the fact that so many different types of ID documents exist. In the U.S., alone, there are more than 1,100 types of official, government-issued credential documents. This one fact renders it virtually impossible to authenticate a document without some form of tool or solution.

How does ID Authentication work?

Modern identity documents are among the most securely produced documents in the world. Great care has been taken to make forgery or alteration of ID documents very challenging. This is achieved by layering security printing techniques and features into the design and production of the document.

Authentication, then, involves testing for the presence of these (and many other) design features to make sure that the document contains the requisite design, printing and security features it should have.

Continued....

Pictured here is just a small sample of the type and nature of security features that might be found on an ID document

The term "forensic" is often used in connection with ID Document Authentication. This is because it may require a unique set of physical tools and objects to perform the level of testing required.

Ultraviolet and/or infrared light, magnification, magnetic detectors, high resolution imagers and more are involved in performing a truly high-confidence physical document authentication.

How is ID Authentication different than Data Verification?

Identity theft is a growing problem in the U.S.; international organized crime groups involved in professional ID forgery have developed data processing tools to efficiently use stolen identity data.

It is easy for organized crime groups to produce or purchase a forged document that contains information that will match the information in the DMV database.

This means that data verification may not detect and prevent fraud performed by more sophisticated operations.

Forensic ID document authentication can be far more difficult to fool. It requires extraordinary skill to produce the dozens of high-tech security printing techniques used to secure ID documents.

Why not do both?

Of course, there is no reason why we should not consider doing both processes — both ID Document Authentication and ID Data Verification. Best-practice would further indicate that when conducting a "remote" transaction where the seller will not physically come to an office for document signing, that a facial-match also should be performed to ensure that the person conducting the sales transaction is, in fact, the person whose face is pictured on the authenticated ID document.

Article provided by contributing author:
Sean Trundy, General Manager
FraudFighter